CLAIMS

1. A combinatorial key-dependent network (46) for encryption/decryption of an input digital data (42) of word size N into an output digital data (44) of the same word size, comprising at least two layers (48), each layer including at least an elementary building block (2), each building block (2) operating on an input block of bits (14, 16) having a word size n+m smaller than or equal to said word size N, for generating an output block of bits (18, 19), characterised in that said building block (2) comprises:

- a multiplexer circuit (4), receiving on a control input (12) a first portion m (14) of said block of bits, for selecting k out of 2^mk key bits on a k-bit output (10) of said multiplexer circuit (4), said first portion (14) of bits being transferred intact to an output (19) of said building block (2); and

- a transformation circuit (6), for transforming a remaining portion n (16) of said input block of bits into transformed bits (18), according to a reversible transformation (R_k) chosen, by means of said selected k bits (10), among a plurality of reversible transformations (R_k) implemented in said transformation circuit (6).

2. A network according to claim 1, wherein adjacent layers (48) are connected by means of a fixed bit permutation block (40).

3. A network according to claim 2, comprising a plurality of fixed bit permutation blocks (40) of the same type.

4. A network according to claim 2, comprising at least two different types of fixed bit permutation blocks (40).

5. A network according to claim 2, wherein bits in said first portion (19) of said block of bits are used, in a next layer, as bits to be transformed (16).

6. A network according to claim 2, wherein, for each building block (2), said first (14) portion of said block

of bits are extracted from at least two building blocks in a preceding layer, provided that m>=2.

7. A network according to claim 2, wherein, for each building block (2), said second (16) portion of said block of bits are extracted from at least two building blocks in a preceding layer, provided that n>=2.

8. A network according to claim 1, wherein each layer (48) comprises at least two building blocks (2).

9. A network according to claim 8, wherein said reversible transformations (R_k) are such that each output bit of said transformed bits (18) is a non-linear function of said first portion (19) of said block of bits and of said k key bits, with the algebraic normal form containing at least one binary product involving both said first portion (19) of said block of bits and said key bits.

10. A network according to claim 9, wherein said reversible transformations (R_k) satisfy a criterion that the uncertainty of n input bits provided by uniformly random k key bits when the output n bits are known is equal to n bits.

11. A network according to claim 1, wherein said multiplexer circuit (4) comprises a lookup table whose content is defined by the key.

12. A network according to claim 1, wherein said transformation circuit (6) comprises XOR gates and controlled switches.

13. A network according to claim 12, wherein each XOR gate has two input bits and one output bit, one of the two input bits being a key bit, and each controlled switch has two input bits, two output bits and one control bit that determines if the input bits are swapped or not, said control bit being a key bit.

14. A network according to claim 13, wherein said multiplexer circuit (4) has two control bits (36), four 3-bit inputs (32) and one 3-bit output (34), and said

transformation circuit (6) comprises two XOR gates (26, 28) and one controlled switch (30).

15. A network according to claim 14, wherein the three bits of said 3-bit output (34) are connected respectively to a first input bit of each XOR gate (26, 28) and to the control bit of said controlled switch (30).

16. A network according to claim 15, wherein a second input bit of each XOR gate (26, 28) is connected to a bit of said second (16) portion of said block of bits.

17. A network according to claim 16, wherein the output bits of said XOR gates (26, 28) are connected to the two input bits of said controlled switch (30).

18. A network according to claim 17, wherein the two output bits of said controlled switch (30) generate the transformed bits (18) of said transformation circuit (6).

19. A network according to claim 1, comprising a plurality of building blocks (2) of the same type.

20. A network according to claim 1, comprising at least two different types of building blocks (2).

21. A network according to claim 1, wherein adjacent layers (48) are connected by means of a block (40') implementing a reversible linear function.

22. A network according to claim 1, wherein two additional input and output keys of word size N are bitwise XORed respectively with said input digital data (42) and with said output digital data (44).

23. A network according to claim 1, wherein said key bits in each layer, having bit size K', are generated from a smaller number of secret key bits, having bit size K, by means of a key expansion algorithm.

24. A network according to claim 23, wherein said K secret key bits are first expanded by means of linear transformations into K' key bits, using a linear code so that any subset of K'' expanded key bits are linearly independent, where K''<=K.

25. A network according to claim 24, wherein said expanded key having bit size K' is used as an input to a further combinatorial key-dependent network of block size K' which is parameterised by a fixed randomly generated key satisfying the condition that every multiplexer implements balanced binary lookup tables.

26. A network according to claim 25, wherein the K' bits produced after every two layers of said further combinatorial key-dependent network are used as said key bits from the multiplexer circuits within the layers of the combinatorial network (46).

27. A network according to claim 25, wherein said further combinatorial key-dependent network comprises a plurality of layers, each layer comprising a plurality of simplified building blocks (50), each building block (50) comprising:

- a multiplexer (54) having one input (58), receiving one control bit (x_3) which is passed to the output (y_3) intact, for selecting one out of two key bits (52) on a one bit output (60);
- a controlled switch 56 having two input bits (x_1, x_2), two output bits (y_1, y_2) and one control bit connected to the output of said multiplexer (60), said control bit determining if said input bits (x_1, x_2) are swapped or not.

28. A block (2) to be used for secret-key-controlled cryptographic functions, operating on an input block of bits (14, 16) for generating an output block of bits (18, 19), characterised in that it comprises:

- a multiplexer circuit (4), receiving on a control input (12) a first portion (14) of m bits of said block of bits, for selecting k out of 2^mk key bits on a k-bit output (10) of said multiplexer circuit (4), said first portion (14) of bits being transferred intact to an output (19) of said building block (2); and
- a transformation circuit (6), for transforming a remaining portion (16) of said input block of bits into transformed bits (18), according to a reversible transformation (R_k) chosen, by means of said selected k

bits (10), among a plurality of reversible transformations (R_k) implemented in said transformation circuit (6).

29. A block according to claim 28, wherein said transformation circuit (6) comprises XOR gates and controlled switches.

30. A block according to claim 29, wherein each XOR gate has two input bits and one output bit, one of the two input bits being a key bit, and each controlled switch has two input bits, two output bits and one control bit that determines if the input bits are swapped or not, said control bit being a key bit.

31. A block according to claim 30, wherein said multiplexer circuit (4) has two control bits (36), four 3-bit inputs (32) and one 3-bit output (34), and said transformation circuit (6) comprises two XOR gates (26, 28) and one controlled switch (30).

32. A block according to claim 31, wherein the three bits of said 3-bit output (34) are connected respectively to a first input bit of each XOR gate (26, 28) and to the control bit of said controlled switch (30).

33. A block according to claim 32, wherein a second input bit of each XOR gate (26, 28) is connected to a bit of said second (16) portion of said block of bits.

34. A block according to claim 33, wherein the output bits of said XOR gates (26, 28) are connected to the two input bits of said controlled switch (30).

35. A block according to claim 34, wherein the two output bits of said controlled switch (30) generate the transformed bits (18) of said transformation circuit (6).

36. A method for encryption/decryption of an input digital data (42) of word size N into an output digital data (44) of the same word size, comprising:

a) dividing said input digital data (42) into blocks of bits (14, 16) each having a word size n+m smaller than said word size N, each block of bits being divided into a first portion m (14) and a second portion n (16);

b) for each block of bits:

b1) addressing a lookup table (4), containing $2^m k$ key bits, by means of said first portion m (14) of bits, for selecting k out of $2^m k$ key bits, transferring intact said first portion m of bits (14) to a first portion of transformed bits (19);

b2) selecting, by means of said selected k bits (10), a reversible transformation (R_k) among a plurality of reversible transformations (R_k);

b3) apply said reversible transformation (R_k) to said second portion n (16) of bits, thus generating a second portion of transformed bits (18).

c) collecting the transformed bits from each block into said output digital data (44).

37. A method according to claim 36, wherein said step b) is reiterated on a block of bits comprising said first (19) and second (18) portion of previously transformed bits.

38. A method according to claim 37, wherein, before each reiteration of step b), a fixed bit permutation (40) is applied to said previously transformed bits.

39. A method according to claim 37, wherein, before each reiteration of step b), a reversible linear function (40') is applied to said previously transformed bits.

40. A data processing device comprising a central processing unit (CPU), volatile or non-volatile memory, and at least a data, instruction or address bus, characterised in that it comprises at least a combinatorial key-dependent network (46), realised according to any of claims 1 to 27, for encryption/decryption of digital data on said data, instruction, or address bus and/or into said memories.

41. A multimedia device for storing and playing copyright digital data characterised in that it comprises at least a combinatorial key-dependent network (46), realised according to any of claims 1 to 27, for encryption/decryption of said copyright digital data.